где $s = \dfrac{НОК(t,\tau)}{t}$, $r \mid t$, $r < t$.

*Следствие 1***.** При выполнении условий теоремы 2 $T(z) \overset{п.н.}{=} НОК(\tau, t)$.

*Следствие 2***.** В случае применения в качестве G_2 LFSR генератора с примитивным характеристическим многочленом период выходной последовательности определяетя следующей формулой:

$$T(z) \overset{п.н.}{=} НОК\left(T(u), \frac{T(v)}{N-1}\right).$$

На основании результатов серии компьютерных экспериментов была выдвинута следующая гипотеза.

Гипотеза. При использовании в качестве G_1 и G_2 LFSR генераторов на различных примитивных характеристических многочленах линейная сложность выходной последовательности $\Lambda(z)$ определяется формулой:

$$\Lambda(z) = \Lambda(u) \cdot \frac{N^{\Lambda(v)} - 1}{N - 1},$$

и для характеристических многочленов исходной и выходной последовательностей верно соотношение: $f_u(x) \mid f_z(x)$.

Также для малых значений был проведен анализ марковости выходной последовательности, который свидетельствует о высоком качестве «запутывания» исходной структуры генератора G_1.

Литература

1. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В*. Основы криптографии. – М.: Гелиос АРВ, 2005.
2. *Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В*. Математические и компьютерные основы криптологии. – Мн.: Новое знание, 2003.

ЗАДАЧА УПРАВЛЕНИЯ РЕГИОНАЛЬНЫМИ СТРУКТУРАМИ

Н. Ю. Костюкович

В работе рассматривается трехуровневая система управления с распределенными источниками информации. Предлагается подход к автоматизации хранения, обработки и быстрой интеграции фрагментов информации в целевую предметную область [1].

Рассмотрим стандартную схему взаимодействия различного типа административных органов в рамках модели Район – Область – Республика (Рис. 1.).

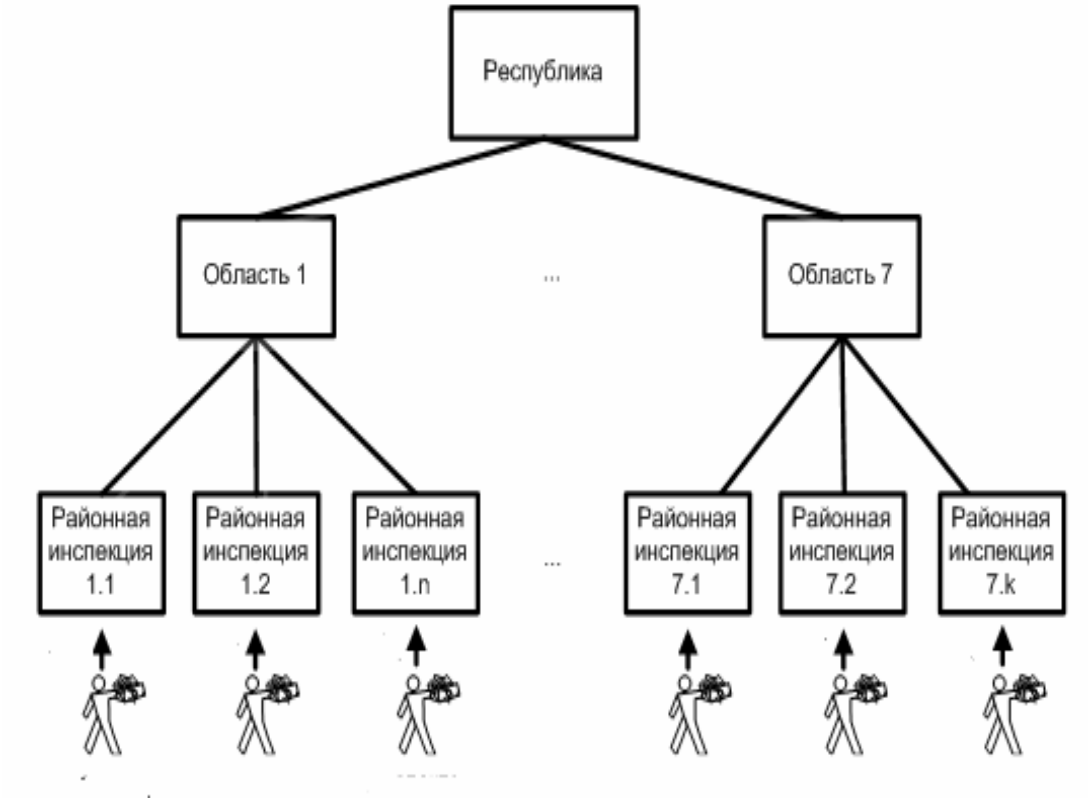

Рис. 1. Схема взаимодействия

Данная схема, как правило, характеризуется:

- большим объемом информации, требуемой для описания каждого из объектов;
- значительным количеством источников исходной информации (134 районные инспекции);
- распределенностью источников по территории республики.

Приведенные выше свойства говорят о возможности выбора многоагентного подхода [2] в качестве концептуальной основы разработки Системы.

Опишем основных участников, участвующих в разработке автоматизированной системы управления.

Одушевленные акторы, участвующие в работе системы известны и находятся на трех уровнях (начиная с первого уровня порождения первичных данных): район (инспекция), область, республика.

Следовательно, в информационно-коммуникативной модели (ИКМ) присутствуют по крайней мере три агента:

$$ИКМ = <aInsp, aObl, aResp>$$

Агент aInsp – реализует процессы решения задач одушевленными акторами на уровне Инспекция. Агент aInsp обеспечивает:

- организацию и ведение БД–i по всем объектам на уровне инспекции,
- обработку всех объектов для получения выходных форм, требуемых на уровне инспекции,
- отсылку всех данных на уровень Область.

Агент aObl – агент, реализующий процессы решения задач одушевленными акторами на уровне Область. Агент aObl обеспечивает:

- формирование и поддержку БД на уровне области,
- получение информации от агента aInsp,
- организацию и ведение БД–o с целью получения необходимых форм на уровне области,
- отсылку всей необходимой информации на уровень Республика.

Агент aResp – реализует процессы решения задач одушевленными акторами на уровне Республика. Агент aResp обеспечивает:

- формирование и поддержку БД на уровне республики,
- получение информации от агента aObl,
- обработку БД–r с целью получения необходимых форм на уровне республики.

Так как информация накапливается и обрабатывается на каждом из трех уровней, то и баз данных соответственно должно быть три. Причем на текущем уровне должна быть доступна информация предыдущих уровней.

Каждый агент реализует процессы, обеспечивающие решение специфической группы задач на каждом уровне с использованием соответствующей информации из базы данных своего уровня. Так как объем информации логически растет по принципу снизу вверх, между агентами необходимо организовать обмен сообщениями двух типов: Сообщение типа 1 (между агентами aInsp и aObl) и Сообщение типа 2 (между агентами aObl и aResp).

Обобщим вышесказанное в форме общей информационно–коммуникативной схемы функционирования Системы (Рис. 2.).

На основе ИКМ были разработаны модели агентов «Район», «Область», «Республика» (Пример модели для уровня «Район» - Рис. 3.) и алгоритмы их взаимодействия. Разработан алгоритм синхронизации данных между агентами различных уровней, а также алгоритм построения входных и выходных форм. Предложены также концептуальные модели посредника для информационного обмена агентов, модель пользователей Системы и модель унифицированного интерфейса. Была разработана подсистема защиты от несанкционированного доступа к данным, а также автоматическое архивирование на случай сбоев и аварийных ситуаций.

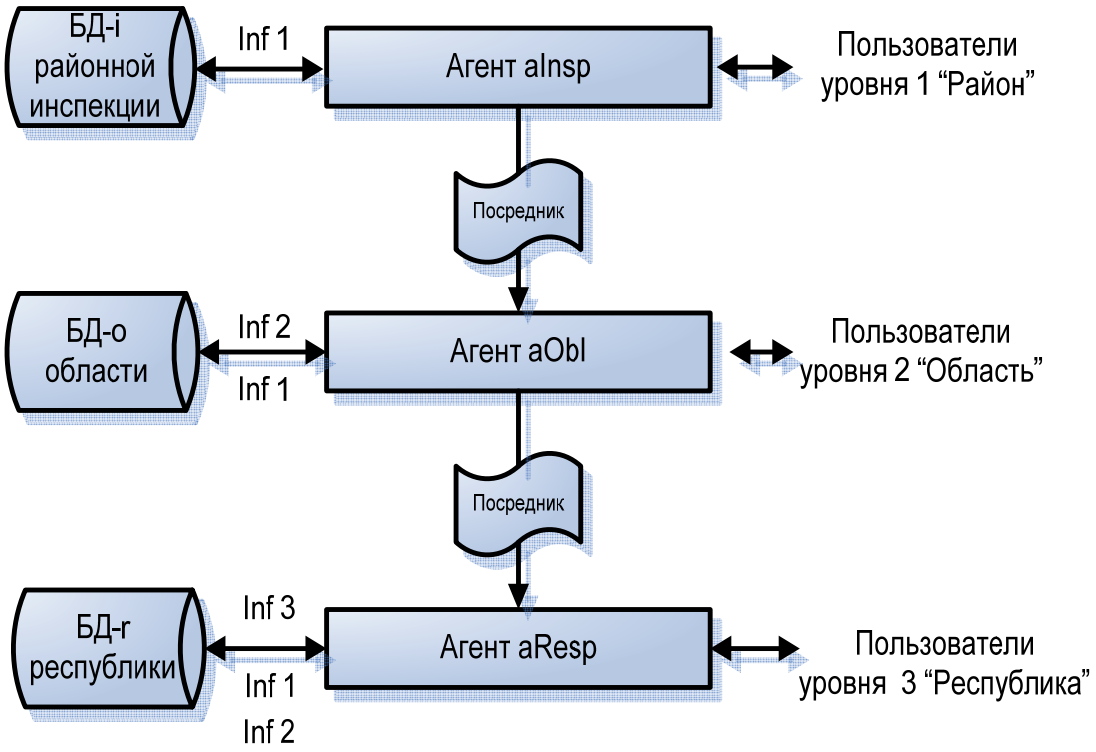

Рис. 2. Информационно-коммуникативная модель

Система реализована с помощью платформы Microsoft .NET и SQL Server 2005.

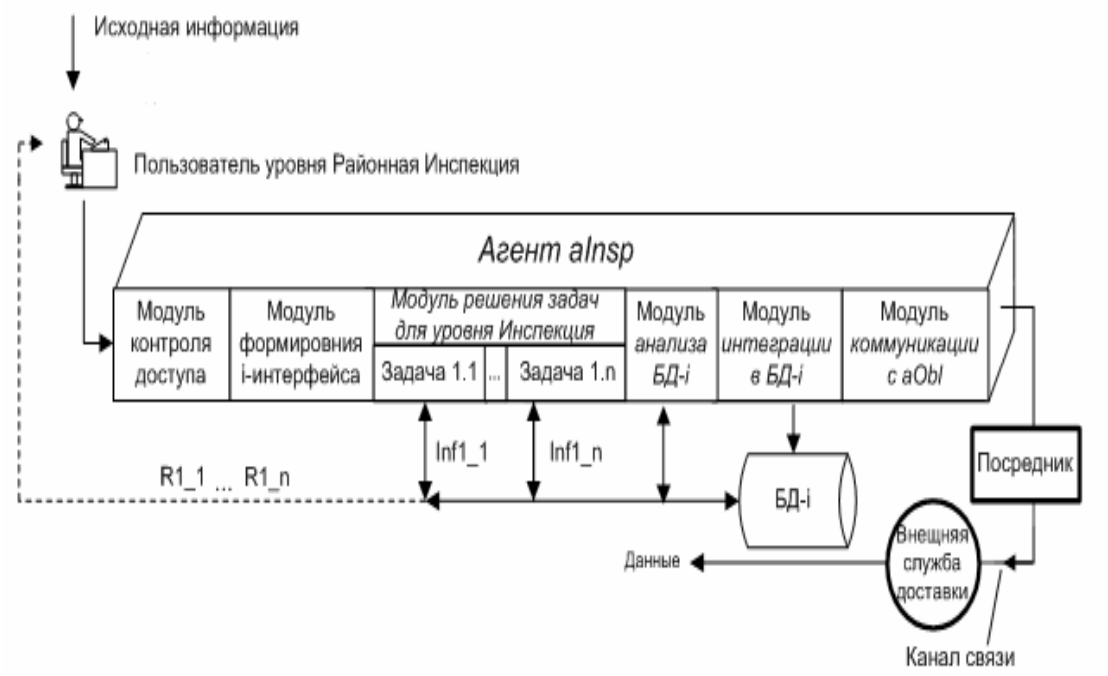

Рис. 3. Модель агента Район

Данный подход применен в одном из административных органов Республики Беларусь.

Литература

1. *Краснопрошин, В.В.* Интеграция распределенных экспертных знаний: проблемы и решения /В.В. Краснопрошин, Г. Шаках, А.Н. Вальвачев // Информатика. – Минск, 2004. – № 1. – С. 45–53.
2. *Katia, P. Sycara* Multiagent Systems /Katia P. Sycara //AI Magazine. – 1998. – Vol. 10, № 2. – P. 79–93.

ЗАДАЧА О СВЕРТКЕ БЕЛКА НА СПЕЦИАЛЬНЫХ ДВУМЕРНЫХ И ТРЕХМЕРНЫХ РЕШЕТКАХ

Е. А. Левина

Одна из важных задач молекулярной биологии заключается в нахождении третичной структуры белка, исходя из информации об его первичной структуре [1, 2]. Напомним, что упорядоченная последовательность аминокислот, из которых состоит белок, называется первичной структурой белка. Под воздействием физиологических условий каждый белок “сворачивается” в уникальную трехмерную структуру, называемую естественной третичной структурой белка. Третичная структура определяет функции, которые белок выполняет в организме. Возникает следующая естественная задача: найти вычислительный метод восстановления третичной структуры белка по известной упорядоченной последовательности аминокислот, ассоциированной с данным белком. В литературе эта задача известна как задача о свертке белка (protein folding problem) [1 – 3].

На практике часто рассматривают упрощенные модели для задачи о свертке белка [4, 5]. Одной из таких моделей является HP-модель, предложенная К. Диллом [5]. В этой модели белок трактуется как последовательность аминокислот, рассматриваемых с точностью до гидрофобичности, а пространство свертки описывается с помощью геометрического графа, ассоциированного с некоторой двумерной или трехмерной решеткой. Свертке белка соответствует инъективное отображение аминокислот в вершины графа, при котором соседние в последовательности аминокислоты соответствуют смежным вершинам графа. Третичная структура белка определяется сверткой, в которой число пар гидрофобных аминокислот, соответствующих смежным вершинам графа и не являющихся соседними членами первичной структуры, максимально. Такие пары называются контактными парами (или просто контактами). В дальнейшем, без ограничения общности будем считать, что белок задан в виде бинарной последовательности, где единицам соответствуют гидрофобные аминокислоты, а нулям – гидрофильные.